Gary M. Hoffman (*Pro Hac Vice*)
Kenneth W. Brothers(*Pro Hac Vice*)
DICKSTEIN SHAPIRO MORIN
& OSHINSKY, LLP
2101 L Street, NW
Washington, DC 20037-1526
Phone (202) 785-9700
Fax (202) 887-0689

Edward A. Meilman (*Pro Hac Vice*)
DICKSTEIN SHAPIRO MORIN
& OSHINSKY, LLP
1177 Avenue of the Americas
New York, New York 10036-2714
Phone (212) 835-1400
Fax (212) 997-9880

Jeffrey B. Demain, State Bar No. 126715
Jonathan Weissglass, State Bar No. 185008
ALTSHULER, BERZON, NUSSBAUM, RUBIN & DEMAIN
177 Post Street, Suite 300
San Francisco, California 94108
Phone (415) 421-7151
Fax (415) 362-8064

Attorneys for Ricoh Company, Ltd.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

SYNOPSYS, INC.,	**CASE NO. C-03-2289-MJJ**
Plaintiff,	
vs.	**DECLARATION OF MICHAEL WEINSTEIN IN SUPPORT OF RICOH'S REPLY IN SUPPORT OF ITS MOTION FOR APPROVAL OF PROTECTIVE ORDER AND SUPPORTING BRIEF**
RICOH COMPANY, LTD.,	
Defendant.	**Date: February 10, 2004** **Time: 9:30 a.m.** **Courtroom: 11**

Michael A. Weinstein declares as follows:

1. My name is Michael A. Weinstein, an attorney with the law firm of Dickstein, Shapiro, Morin & Oshinsky, LLP, counsel for Ricoh Company Limited ("Ricoh"). I am over the age of 21 and am competent to make this declaration. Based on my personal knowledge and information, I hereby declare to all the facts in this declaration.

2. Attached hereto as Ex. 1 is a true and correct copy of a letter from E. Meilman to E. Moller dated November 20, 2003.

3. Attached hereto as Ex. 2 is a true and correct copy of a letter from E. Moller to E. Meilman dated December 7, 2003.

4. Attached hereto as Ex. 3 is a true and correct copy of the Declaration of Van Q. Nguyen in support of Synopsys' Opposition to Ricoh's Motion for Entry of Protective Order dated January 20, 2004.

5. Counsel for Ricoh met and conferred with counsel for Synopsys in November, 2003 and discussed the number of experts allowable under the protective order and agreed on three (3) experts.

6. The Government Contracts group within Dickstein Shapiro Morin and Shapiro, LLP deals with many government bid protests, adversarial proceedings, litigation involving confidential material. The group has received confidential material pursuant to protective orders and maintained that material within a locked facility within the firm. To date, no confidential material received by the Government Contracts group under a protective order has been lost or stolen.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Signed at Washington, D.C. on January 27, 2004.

/s__ Michael A. Weinstein_
Michael A. Weinstein

EX,lIBIT 1

DICKSTEIN SHAPIRO MORIN & OSHINSKY LLP

1177 Avenue of the Americas • New York, NY 10036-2714
Tel (212) 835-1400 • Fax (212) 997-9880

Writer's Direct Dial: (212) 896-5471
E-Mail Address: MeilmanE@dsmo.com

November 20, 2003

BY FACSIMILE AND U.S. MAIL

Erik K. Moller, Esq.
Howrey Simon Arnold & White, LLP
301 Ravenswood Avenue
Menlo Park, CA 94025-3434

Re: *Synopsys, Inc. v. Ricoh Company, Ltd.*
Case No. CV 03-02289 MJJ

Ricoh Company, Ltd. v. Aeroflex Inc., et al.
Case No. CV 03-04669 MMJ
Our Ref.: R2180.0171

Dear Erik:

With regard to the protective order, we believe that the following additional provision recording source code is appropriate:

Unless otherwise ordered by the Court or permitted in writing by the producing party, all source code produced or exchanged in the course of this litigation shall be Confidential Information and access thereto shall be limited to the outside attorneys of record for the parties in this litigation and employees of such attorneys to whom it is necessary that the material be shown for the purposes of this litigation and not more than three (3) outside experts who have signed an undertaken pursuant to paragraph 5 but only after compliance with the provision of paragraph 5. Any notes or other information created as a consequence of such access shall also be Confidential Information under this protective order. Working copies of the source code shall be maintained by the receiving party in a secure facility which, in the case of Synopsys means Synopsys' Secured User Research Facility (SURF) and in the case of Ricoh, means a locked office at the law firm of Dickstein Shapiro Morin & Oshinsky, LLP and which contains a computer which is not a part of any network and on which the source code can be loaded.

We believe that the secured facility we are offering is even more secure that Synopsys' SURF facility.

Very truly yours,

Edward A. Meilman

EAM/rra

cc: Gary Hoffman, Esq.
Kenneth Brothers, Esq.
Jeffrey Demain, Esq.

EXHIBIT 2

HOWREY SIMON ARNOLD & WHITE
HOWREY LLP
ATTORNEYS AT LAW

301 RAVENSWOOD AVENUE
MENLO PARK, CA 94025-3434
PHONE 650.463.8100
FAX 650.463.8400
A LIMITED LIABILITY PARTNERSHIP

December 7, 2003

VIA FACSIMILE AND U.S. MAIL

Edward A. Meilman
Dickstein Shapiro Morin & Oshinsky, LLP
1177 Avenue of the Americas
New York, NY 10036-2714

Re: *Synopsys, Inc. v. Ricoh Company, Ltd.*,
Case No. C 03-2289 MJJ

Dear Ed:

This letter follows our discussion during the meet and confer teleconference on December 1, 2003 regarding the terms for the production of the source code for Synopsys' Design Compiler product in this action.

We stated that Synopsys could make arrangements at one of its East Coast facilities to provide Ricoh with more convenient access to the source code for Synopsys' Design Compiler product. You asked us to inquire as to the conditions for the production of the source code at such a facility. Synopsys can make arrangements to provide you with a secured location at its facility in Bethesda, Maryland. We would provide a computer that would be loaded with the source code to be produced by Synopsys and suitable software for review of this code. Synopsys will allow Ricoh to make hardcopy of specific portions of the source code. The hardcopy can then be reviewed, pursuant to the protective order, outside of the facility. You would have access to the Bethesda facility during regular business hours without need to make any special arrangements.

In addition, we continue to offer the use of Synopsys' SURF facility at its campus in Mountain View, at which you would have 24/7 access.

Very truly yours,

Erik K. Moller

EKM:gg
cc: Gary M. Hoffman
Jeffrey B. Demain

HOWREY SIMON ARNOLD & WHITE
HOWREY LLP
WHERE LEADERS GO™

301 RAVENSWOOD AVENUE
MENLO PARK, CA 94025-3434
PHONE: 650.463.8100 • FAX: 650.463.8400

FACSIMILE COVER SHEET

DATE: December 7, 2003

TO:

1. NAME: Edward A. Meilman COMPANY: Dickstein Shapiro, et al.
CITY: New York, NY FAX #: (212) 997-9880 PHONE #: (212) 835-1400

2. NAME: Gary M. Hoffman COMPANY: Dickstein Shapiro, et al.
CITY: Washington, DC FAX #: (202) 887-0689 PHONE #: (202) 785-9700

3. NAME: Jeffrey Demain COMPANY: Altshuler, Berzon, Nussbaum, Rubin
CITY: San Francisco, CA FAX #: (415) 362-8064 PHONE #:

4. NAME: COMPANY:
CITY: FAX #: PHONE #:

5. NAME: COMPANY:
CITY: FAX #: PHONE #:

FROM: NAME: Erik Moller, Esq.

DIRECT DIAL NUMBER: (650) 463-8175 USER ID: 5172

NUMBER OF PAGES, INCLUDING COVER: 2 CHARGE NUMBER: 06816.0061.000000

☒ **ORIGINAL WILL FOLLOW VIA:**

☒ REGULAR MAIL ☐ OVERNIGHT DELIVERY ☐ HAND DELIVERY ☐ OTHER:

☐ **ORIGINAL WILL NOT FOLLOW**

SUPPLEMENTAL MESSAGE:

THE INFORMATION CONTAINED IN THIS TRANSMISSION IS PRIVILEGED AND CONFIDENTIAL. IT IS INTENDED ONLY FOR THE USE OF THE INDIVIDUAL OR ENTITY NAMED ABOVE. IF THE READER OF THIS MESSAGE IS NOT THE INTENDED RECIPIENT, YOU ARE HEREBY NOTIFIED THAT ANY DISSEMINATION, DISTRIBUTION OR COPYING OF THIS COMMUNICATION IS STRICTLY PROHIBITED. IF YOU HAVE RECEIVED THIS COMMUNICATION IN ERROR, PLEASE NOTIFY US IMMEDIATELY BY TELEPHONE AND RETURN THE ORIGINAL MESSAGE TO US AT THE ABOVE ADDRESS VIA THE U.S. POSTAL SERVICE. THANK YOU.

EXHIBIT 3

Teresa M. Corbin (SBN 132360)
Christopher Kelley (SBN 166608)
Thomas C. Mavrakakis (SBN 177927)
Erik K. Moller (SBN 147674)
HOWREY SIMON ARNOLD & WHITE, LLP
301 Ravenswood Avenue
Menlo Park, California 94025
Telephone: (650) 463-8100
Facsimile: (650) 463-8400

Attorneys for Plaintiff SYNOPSYS, INC.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

SYNOPSYS, INC.,

Plaintiff,

vs.

RICOH COMPANY, LTD.,

Defendant.

Case No. CO3-02289 MJJ

DECLARATION OF VAN Q. NGUYEN IN SUPPORT OF SYNOPSYS' OPPOSITION TO RICOH'S MOTION FOR ENTRY OF PROTECTIVE ORDER AND CROSS-MOTION FOR ADOPTION OF SYNOPSYS' PROTECTIVE ORDER AND DISCOVERY PROCEDURES

Date: February 10, 2004
Time: 9:30 a.m.
Ctrm: 11

I, Van Q. Nguyen, hereby declare as follows:

1. I currently serve as Director of IT Security at Synopsys, Inc. ("Synopsys"), a position I have held since October 14, 2002. I joined Synopsys in October 14, 2002. Prior to that I held positions I worked as director of IT security at APL for about two and half years, at Fidelity Investments for two years and at Nokia for five years, all in the area of IT and corporate security. The matters set forth in this declaration are based upon my personal knowledge, except where otherwise indicated, and if called as a witness, I could and would testify competently thereto.

2. As Director of IT Security, I manage the security group within Synopsys' Information Technology department, which employs a total of five persons (myself included), all of whom are computer security professionals and dedicated to security-issues at Synopsys. Additionally, all of the IT department, which includes approximately 168 employees and contractors, help support security

functions. Synopsys spends approximately 20% of its annual IT budget on IT security. One of my most important responsibilities as Director of IT Security is to ensure that only authorized persons can have access to Synopsys source code and other highly confidential engineering information stored on Synopsys' servers. To achieve this, Synopsys has established a policy and standards to provide for the comprehensive protection for all Synopsys private and proprietary information assets. These policies and standards are designed to ensure that electronic access to Synopsys' proprietary information, including its source code, are tightly controlled. The security of Synopsys' source code rests on the fact that the code resides only in the closed network of Synopsys' computers, and that only authorized users are able to access this computer network. The source code for Synopsys' logic synthesis products is managed using the ClearCase® software asset management tool. This tool, and the source code that it manages, reside on Synopsys' internal computer network. Users obtain access to the source code through the ClearCase® tool. In order, therefore, to review or edit the code, authorized users connect through the Synopsys computer network to the ClearCase® server, which then provides them with access to the code sections that they need.

3. Synopsys ensures the security of its source code by imposing tight restrictions on who may access the source code and by deploying a multi-layer security approach that ensures that only authorized individuals are able to access the ClearCase® server that provides access to the source code. That multi-layer security approach includes (a) network perimeter protection measures, (b) internal network segmentation and security measures, (c) per-system authentication, and a (d) specialized remote access environment. With respect to (a), we have established a firewall controlling all access from outside the Synopsys IT environment to the inside of the environment that includes three layers of antivirus protection, and intrusion detection systems. These measures limit the ability of outsiders without physical access to our network environment to damage and/or access our facilities. With respect to (b), the IT environment is segmented to control inter-facility access. This means that in order to access servers at one Synopsys facility from another facility, a user is required to provide a password that authenticates them as someone with authority to access one segment of the Synopsys network from another. Some portions of the Synopsys network are actually physically isolated from the remainder so that it is impossible to use them to access other portions of the network. Portions of

the network used by customers and for teaching purposes are isolated in this manner. With respect to (c), each computer on our network requires password-based logon access. In addition, all portable computers have been individually equipped with a personal firewall and additional antivirus software. Once a user has been authenticated as someone authorized to use a given computer, access to sensitive data and systems, such as the ClearCase® source code repository, requires additional, separate authentication, by way of a separate password identifying the user as someone authorized to access this sensitive data.

4. In addition to the network security provisions described above, Synopsys' computer network is further secured by the fact that physical access to each of Synopsys' engineering facilities is strictly controlled. Employees or contractors entering any Synopsys facility are required to display a badge or prove their authority to enter by use of a coded card and PIN. Once within the physical confines of a Synopsys facility, even if users have access to a computer located within that facility, they cannot access Synopsys' engineering materials on the computer network until they provide a password that authenticates them as someone who is entitled to have access to those materials.

5. Synopsys also allows a limited number of personnel to access the Synopsys engineering computer network remotely using a virtual private network (VPN) set up across remote dial-in telephone lines and/or across the internet between the physically secured Synopsys computer network and an authorized user's remote computer. The specialized remote access environment referred to above as element (d) of the Synopsys security plan ensures that this remote access is secure. Synopsys uses a VPN client software constructed by Synopsys' IT security group exclusively for use with our VPN. All communications through the VPN are secured by means of industrial grade (128 bit or greater) encryption of all data passed between the secured Synopsys network and the remote computer.

6. In order to access the Synopsys network remotely, a Synopsys employee or agent must submit an application. If the application is approved by network administrators, the employee or agent is given a SecurID® token manufactured by RSA Security, Inc. This token is a piece of circuitry, contained within either a key fob housing or a credit-card sized package, that generates and displays a new access code every 60 seconds. The user combines a PIN that is personal to them with the code displayed on the SecurID® token. This allows the system to authenticate that the person requesting

access is in possession, in real-time, of the SecurID® token issued to an authorized user and that this person knows a PIN that identifies them as the authorized user to whom the SecurID® token was issued. Once a user has accessed the network using their SecurID® token and PIN, they still must provide additional authentication to access more highly sensitive portions of the network, such as the ClearCase software asset management tool.

7. In order to ensure the continuing robustness of the security measures taken by my IT security department, we regularly use vulnerability analysis assessment tools to provide us with advanced notice of any potential defects in network security. In addition, we hire outside vendors to perform penetration analyses and to give us independent assessments of the effectiveness of our security measures.

8. Someone from my IT security staff is on call around the clock to ensure that we can respond promptly to any potential security issues that may arise. Our network includes elements that are designed to detect unusual activity and will page or otherwise alert personnel from my team to the existence of any potential developing security breach. We maintain a close working relationship with the persons responsible for security of Synopsys' physical plant so that we can make joint response to any potential threat. In addition, we conduct security awareness training for our employees and operate an intranet site on Synopsys' network dedicated to IT security issues.

9. To my knowledge, our efforts to secure access to Synopsys' engineering materials have been successful to date. I am not aware of any instance where unauthorized copies of Synopsys engineering source code were withdrawn from the secured Synopsys computer network.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. This declaration was executed in Mountain View, California on January 20, 2004.

Van Q. Nguyen